



# Sharing and Protecting Data to Improve Student Outcomes

Community Schools Community of  
Practice

Nov. 16, 2017



# Agenda

- **Why sharing and protecting student data matters**
- Sharing data deep dive
- Protecting data deep dive
- Tips and best practices
- Questions and next steps



# Why Sharing and Protecting Student Data Matters



# Why Sharing and Protecting Student Data Matters

- OSSE is committed to **providing our students and families** with an excellent education and **sustaining, accelerating, and deepening** the progress being made in DC education.
- OSSE has committed to providing **high-quality, actionable data** as one of four key priorities in its strategic plan.
- As DC's state education agency, OSSE plays an important role in ensuring student information remains **private and protected**.
- OSSE has taken a **robust approach** to codifying policies and procedures to protect student information and to build the agency's capacity around data privacy and security.



# Why Privacy Matters

## What are examples of student data that you use?

Student name	Disability status
Date of birth	IEP
Parent name and contact information	English Learner
Race/ethnicity	Bus route
Gender	Assessment outcomes
Attendance	Discipline
Unique student identifier	Social Security number
Courses taken	Grades

**91,394 students were enrolled in DC in the 2016-17 school year. Schools collect student-level data on each of these students.**



## Sharing Data Deep Dive



**Personally Identifiable Information (PII)** is information that, alone *or in combination*, can be linked to a specific student including but not limited to:

- Name of student, parents, or other family members
- Address of student, parents, or other family members
- Personal identifier, e.g., Social Security Number, unique student identifier, biometric record
- Indirect identifiers, e.g. date of birth, place of birth, mother's maiden name



## Personally identifiable information continued:

- **Aggregate data generally does not include** personally identifiable information.
- However, sometimes the sample underlying aggregate data is so **small and/or narrowly-defined** that the recipient could easily identify the student. Examples include but are not limited to:
  - Special education data about a school that has only a small number of special education students
  - Certain types of aggregate counts of zero students or percentages of 0 or 100%
  - Two separate files that when combined can be used to link information to a student





# Sharing Data Deep Dive

**Disclosure** means to provide access to personally identifiable information by any means, including oral, written, or electronic, to any party except the party that provided or created the record.

**Re-disclosure** is when information is disclosed to a third party, and the third party then provides that information to another entity. This can be authorized or unauthorized.



**Authorized disclosure** or re-disclosure is the permitted sharing of information with a third party. Schools are typically authorized to disclose data for reasons that include:

- Pursuant to parent or student rights under FERPA
- Research study
- Audit or evaluation
- Directory information
- School official with legitimate educational interest

**Unauthorized disclosure** or re-disclosure is the sharing of information with a third party that is not permitted.



**Data sharing agreements** are legal documents between two or more parties that codify the terms and conditions for the sharing and use of the data.

They are best practice and required under FERPA when sharing personally identifiable information with authorized representatives. They should address:

- The relationship between the parties sharing and receiving data
- Exact data elements being shared
- Explicit purpose(s) for which the information is being shared
- Timeline and method for data destruction

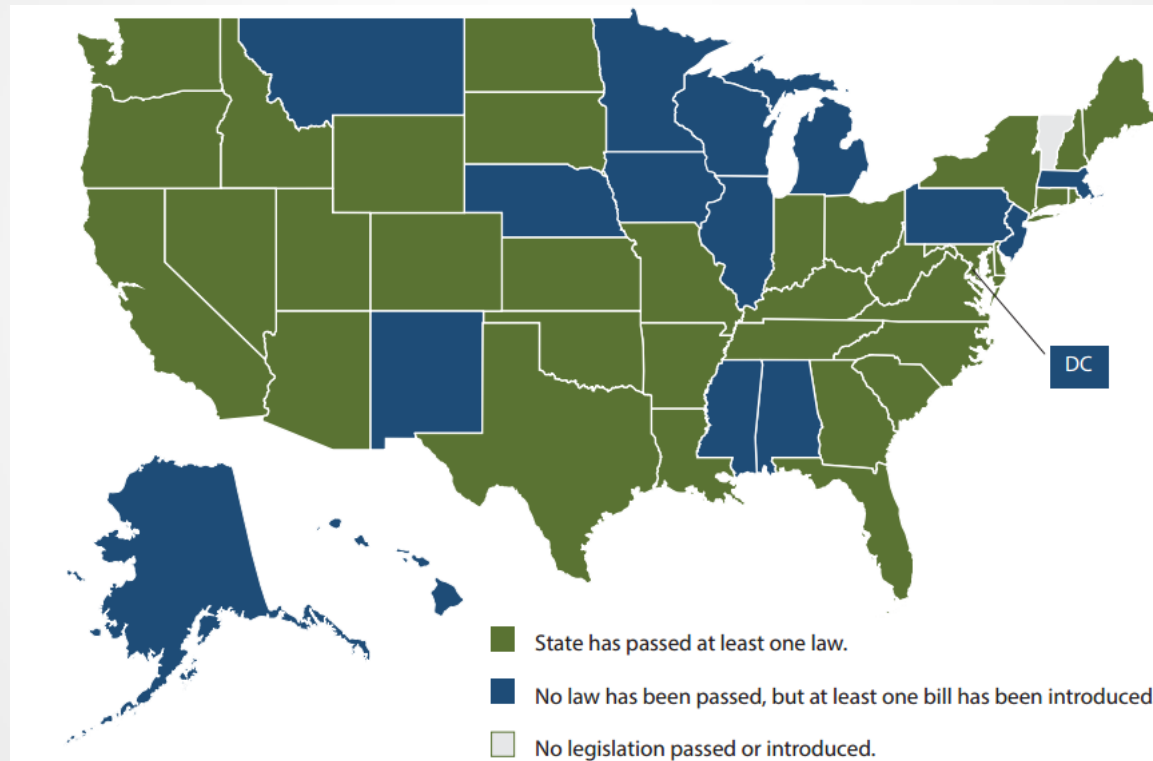


## Protecting Data Deep Dive



# Protecting Data Deep Dive

- In 2015, **48 states** introduced 187 student privacy bills.
- **34 states** have passed 53 student privacy laws since 2013.



Source: Vance, Amelia. Policymaking on Education Data Privacy: Lessons Learned. Alexandria, VA: NASBE, Apr. 2016.



# Protecting Data Deep Dive

- Of the hundreds of laws that have been introduced, very few address the importance of **training**.
- However, human error is a factor in **95 percent** of all data security incidents according to IBM's 2014 Cyber Security Intelligence Index.



# Protecting Data Deep Dive

Student Privacy 101: FERPA for Parents and Students

**THE FAMILY  
EDUCATIONAL  
RIGHTS AND  
PRIVACY  
ACT = FERPA**

An illustration depicting the components of FERPA: a gavel on a block, a family of three (a man with glasses, a woman, and a child), a man pointing upwards, a red banner with the word 'PRIVACY' written on it, a school building, three large blue dollar signs, and the U.S. Capitol building. The video player interface at the bottom shows a progress bar at 0:14 / 4:03, a play button, a volume icon, a CC icon, a settings gear, the YouTube logo, and a full screen icon. An 'Exit full screen' button is also visible in the top right corner of the video frame.

<https://youtu.be/nhIDkS8hvMU>



# Protecting Data Deep Dive

Schools routinely receive requests for a variety of information through several channels:

- FOIA
- FERPA
- Data requests
- Media inquiries
- Community based organizations

**The Family Educational Rights and Privacy Act (FERPA) applies to all of these.**





FERPA gives parents and students over 18 these basic rights:

- The right to **inspect and review** the student's education records maintained by the school
- The right to request that a school **amend** the student's education records
- The right to **consent** in writing to the disclosure of personally identifiable information from the student's education record, except under certain permitted situations
- The right to **file a complaint** with the Family Policy Compliance Office (FPCO) regarding an alleged violation under FERPA



# Protecting Data Deep Dive

Personally identifiable information can only be disclosed under FERPA in two circumstances:

- **Obtain the prior, written consent** of the parent/student over 18
- Ensure that the re-disclosure falls under a **FERPA exception** and make a record of the re-disclosure



## Student Privacy Tips and Best Practices

- Data Sharing Guideline
- Data Privacy tips and Best Practices



# Summary of Data Sharing Guidelines

## **Before sharing information, first ask yourself:**

- Am I sending the minimum amount of information necessary to do my job?
- Could it be linked to an individual student or child?
- If so, could this information be provided in aggregate or de-identified?



# Summary of Data Sharing Guidelines

## **If aggregate data can be provided, ask yourself:**

- For redactions, is all PII deleted?
- Have I sanitized and removed metadata from documents?
- Have I checked all worksheets/tabs for PII when working with spreadsheets?
- Have I had someone else review to ensure there is no PII?



# Summary of Data Sharing Guidelines

## **If the information does include PII, ask yourself:**

- Who is receiving this information, and do they have a right to have it?
- How can I transmit it securely?
- Have I marked the data as confidential?



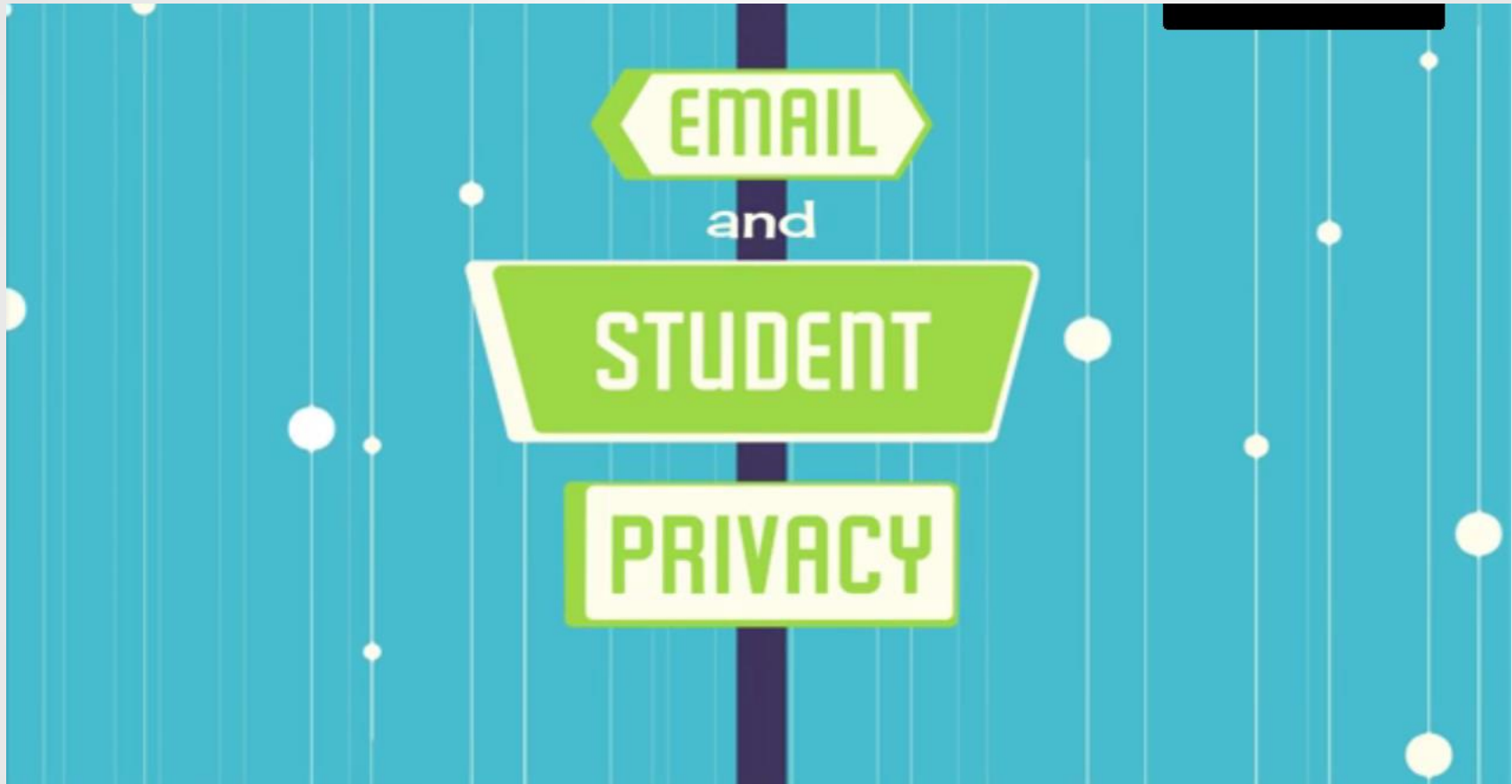
# Data Privacy Tips and Best Practices

Protecting student data, including complying with federal law, entails implementing best practices, including but not limited to:

- Send personally identifiable information via **secure platforms** like:
  - Secure data systems
  - Secure file sharing sites like Upload.Dc.gov, SFTP, and shared drives
  - Phone, mail, and in-person delivery
- When **sending emails**, consider:
  - Limit/redact information whenever possible
  - Be careful when using BCC or consider sending separate emails
  - Add *Confidential* to the subject line and insert language in the signature that this information is protected



# Email and Student Privacy



<https://youtu.be/hm82nRxi0yg>





# Data Privacy Tips and Best Practices

- Be careful with **equipment** like laptops, smartphones, and thumb drives
- Ensure equipment is **password-protected**
- Use **trusted Wi-Fi** for sensitive activities
- Protect **visibility of reports** and computer monitors when displaying and working with confidential information
- Lock or shut down **workstations** when left unattended for any amount of time
- Store data in a **secure location**. Physical data should be protected from unauthorized persons, or locked away when not in use
- Shred and/or **destroy paper** and electronic files when no longer needed



# Data Privacy Tips and Best Practices

- Do not share **passwords** with anyone, and only authorized staff members should use their designated user accounts
- Do not **fax or print** confidential data unless the area is secured



## Questions and Next Steps

- Forthcoming Guidance and Ongoing Training
- Contact Information
- Next Steps



**Everyone plays an important role in protecting sensitive data. Never guess about data privacy, FERPA requirements, or technical security of records that contain PII.**

## **Additional Resources**

- U.S. Department of Education [Protecting Student Privacy](#)
- Data Quality Campaign [A Stoplight for Student Data Use](#)



# Stay in Touch

## FIND US

### ADDRESS:

1050 First St., NE  
Washington, DC 20002

### POC:


William Henderson  
[William.Henderson@dc.gov](mailto:William.Henderson@dc.gov)


Elizabeth Laird  
Elizabeth. [Laird@dc.gov](mailto:Laird@dc.gov)

## GET SOCIAL

 [facebook.com/ossedc](https://facebook.com/ossedc)

 [twitter.com/ossedc](https://twitter.com/ossedc)

 [youtube.com/DCEducation](https://youtube.com/DCEducation)

 [www.osse.dc.gov](http://www.osse.dc.gov)



| Thank you!